Journal of Number Theory 131 (2011) 1808–1823

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

# Infinite class of new sign ambiguities

Heon Kim [a,*], Paul van Wamelen [b], Helena A. Verrill [c]

[a] Department of Natural Sciences, Southern University at New Orleans, 6801 Press Dr., New Orleans, LA 70126, United States
[b] American Institutes for Research, 1000 Thomas Jefferson St., Washington, DC 20007, United States
[c] Department of Mathematics, Louisiana State University, Baton Rouge, LA 70803, United States

ARTICLE INFO

*Article history:*
Received 17 March 2009
Revised 31 January 2011
Accepted 23 March 2011
Available online 19 May 2011
Communicated by David Goss

*Keywords:*
Gauss sum
Stickelberger's theorem
Sign ambiguity

ABSTRACT

In 1934, two kinds of multiplicative relations, *the norm and the Davenport–Hasse* relations, between Gauss sums, were known. In 1964, H. Hasse conjectured that the norm and the Davenport–Hasse relations were the only multiplicative relations connecting Gauss sums over $\mathbb{F}_p$. However, in 1966, K. Yamamoto provided a simple counterexample disproving the conjecture. This counterexample was a new type of multiplicative relation, called a *sign ambiguity*, involving a $\pm$ sign not connected to elementary properties of Gauss sums. In this paper, we give an explicit product formula involving Gauss sums which generates an infinite class of new sign ambiguities, and we resolve the ambiguous sign by using Stickelberger's theorem.

Published by Elsevier Inc.

## 1. Introduction

A *Gauss sum* is a particular kind of finite sum of roots of unity. The general theory of Gauss sums was developed in the early nineteenth century, with the use of Jacobi sums and their prime decomposition in cyclotomic fields.

Let $e > 2$ be a positive integer, and $p$ a prime number such that $p \equiv 1 \pmod{e}$. Let $\mathbb{F}_p$ be the finite field with $p$ elements, $\gamma$ a generator of the cyclic multiplicative group $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\} = \{\gamma^k \colon 0 \leqslant k \leqslant p-2\}$. For any positive integer $n$, denote by $\zeta_n$ a fixed primitive $n$-th root of unity. Let $\chi$ be

* Corresponding author.
*E-mail addresses:* hkim@suno.edu (H. Kim), wamelen@math.lsu.edu (P. van Wamelen), verrill@math.lsu.edu (H.A. Verrill).
*URL:* http://www.sunocas.com/kim/ (H. Kim).

0022-314X/$ – see front matter Published by Elsevier Inc.
doi:10.1016/j.jnt.2011.03.005

the multiplicative character on $\mathbb{F}_p$, defined by $\chi(\gamma^k) = \zeta_e^k$ (for any integer $k$) and $\chi(0) = 0$. For any integer $a \in \mathbb{Z}$, the Gauss sum $\tau(a)$, associated with $\chi^a$ is defined by

$$\tau(a) = \sum_{t \in \mathbb{F}_p} \chi^a(t)\zeta_p^t.$$

If $a \not\equiv 0 \pmod{e}$, then $|\tau(a)| = p^{1/2}$ [1, Theorem 1.1.4]. A multiplicative relation between Gauss sums is a relation of the form $\prod_{a=1}^{e-1} \tau(a)^{c_a} = \eta$, where the $c_a \in \mathbb{Z}$ and $\eta$ is a unit in $\mathbb{Q}(\zeta_e)$. The fundamental multiplicative relations are:

The norm relation: for $a \not\equiv 0 \pmod{e}$,

$$\tau(a)\tau(-a) = \chi^a(-1)p. \tag{NR}$$

The Davenport–Hasse product formula: for integers $m, n > 1$ such that $e = mn$ and for $1 \leqslant t \leqslant m-1$,

$$\chi^{tn}(n)\frac{\tau(t)}{\tau(tn)}\prod_{k=1}^{n-1}\frac{\tau(km+t)}{\tau(km)} = 1. \tag{DH}$$

H. Hasse [3, p. 465] conjectured that all the multiplicative relations between Gauss sums can be deduced from these two relations. But, K. Yamamoto [8] gave a counterexample amounting to a sign ambiguity of the type

$$\prod_{a=1}^{e-1} \tau(a)^{c_a} = u_p \zeta_e^k, \tag{SA}$$

where $u_p \in \{\pm 1\}$ cannot be determined by the elementary properties of Gauss sums, the norm relation, and the Davenport–Hasse formula. Yamamoto also determined the structure of the module generated by all multiplicative relations modulo those generated by the norm and Davenport–Hasse relations. He showed that, for any integer $e \geqslant 3$, there are exactly $2^{r-1} - 1$ multiplicatively independent sign ambiguities of the type (SA), where $r$ is the number of distinct prime divisors of $e$ (resp. of $\frac{e}{2}$) if $e \not\equiv 2 \pmod{4}$ (resp. if $e \equiv 2 \pmod{4}$).

In 2007, B. Murray [5] gave an infinite class of sign ambiguities when $e = q_1q_2$, where $q_1$ and $q_2$ are prime numbers such that $q_1 \equiv 5 \pmod{8}$, $q_2 \equiv 3 \pmod{4}$ and $q_2$ is a biquadratic residue modulo $q_1$.

In the present paper, the authors give an infinite class of multiplicative relations between Gauss sums, in the case $e = 4q$ where $q$ is a prime number such that $q \equiv 7 \pmod{8}$, yielding exactly one sign ambiguity for every prime $p$, not deducible from (NR) and (DH), resolved using Stickelberger's theorem.

## 2. Yamamoto's sign ambiguities

### 2.1. Half-sets

For any positive integers $i$ and $a$, let

$$L_i(a) = \text{least nonnegative integer in } i\mathbb{Z} + a.$$

**Definition 1.** Fix $G = (\mathbb{Z}/e\mathbb{Z})^\times$ with an order 2 binary operation $a \mapsto -a$. For $H \subset G$, let $-H = \{-a \mid a \in H\}$. A *half-set* $H$ of $G$ is a subset of $G$ such that $H \cup (-H) = G$ and $H \cap (-H) = \emptyset$.

**Definition 2.** Let $\phi_1$ and $\phi_2$ be the natural maps

$$\phi_1 : G = (\mathbb{Z}/e\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times \quad \text{by } \phi_1(a) = a \pmod 4,$$
$$\phi_2 : G = (\mathbb{Z}/e\mathbb{Z})^\times \to (\mathbb{Z}/q\mathbb{Z})^\times \quad \text{by } \phi_2(a) = a \pmod q.$$

**Definition 3.** We will denote subsets of $(\mathbb{Z}/4\mathbb{Z})^\times$ and of $(\mathbb{Z}/q\mathbb{Z})^\times$ by Roman capital letters (possibly with subscripts), and the corresponding preimages under $\phi_1$ and $\phi_2$ respectively by the corresponding bold face capital letter. For example, for $A \subset (\mathbb{Z}/q\mathbb{Z})^\times$, we define

$$\mathbf{A} = \left\{ g \in G \;\middle|\; \phi_2(g) \in A \right\}.$$

**Remark 4.** Note that the set of all quadratic residues modulo a prime number $q$ can be a half-set of $(\mathbb{Z}/q\mathbb{Z})^\times$ when $q \equiv 3 \pmod 4$ and that $\mathbf{K}_1$ and $\mathbf{K}_2$ are also half-sets of $G$.

Throughout the paper, let $K_1$ (resp. $K_2$) be the set consisting of the quadratic residues modulo 4 in $(\mathbb{Z}/4\mathbb{Z})^\times$ (resp. modulo $q$ in $(\mathbb{Z}/q\mathbb{Z})^\times$), and fix $K_1$, $K_2$ and $\mathbf{K}_2$ as the half-sets of $(\mathbb{Z}/4\mathbb{Z})^\times$, $(\mathbb{Z}/q\mathbb{Z})^\times$ and $G$ respectively.

Let $O$ and $E$ be the sets of odd and even numbers in $K_2$ respectively, and let

$$I_1 = \left\{ t \in K_2 \;\middle|\; 1 \leqslant t \leqslant \frac{q-1}{2} \right\}, \qquad I_2 = \left\{ t \in -K_2 \;\middle|\; 1 \leqslant t \leqslant \frac{q-1}{2} \right\},$$
$$I_3 = I_1 \cup I_2, \qquad M_1 = \left\{ t \in K_2 \;\middle|\; \frac{q+1}{2} \leqslant t \leqslant q-1 \right\}.$$

Let $S = \#(\mathbf{K}_1 \cap (-\mathbf{K}_2))$, $m_1 = \#M_1$, and $n_1 = \#O$. For the remainder of this paper, we fix $n_0$ to be a rational number, defined as follows

$$n_0 = \frac{1}{2}(S + m_1 + n_1) - \frac{3\phi(e)}{8}.$$

In Proposition 9 we will see that $n_0$ is in fact an integer. In order to show this, we first need a few lemmas.

**Example 5.** Suppose $q = 7$, so $e = 28$. Then

$$(\mathbb{Z}/28\mathbb{Z})^\times = \{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\}.$$

Thus we have

$$K_1 = \{1\}, \qquad K_2 = \{1, 2, 4\},$$

where all numbers are understood to be taken modulo the appropriate integer, i.e., 4 and 7 respectively. With these choices of $K_1$ and $K_2$, we have

$$\mathbf{K}_1 = \{1, 5, 9, 13, 17, 25\}, \qquad \mathbf{K}_2 = \{1, 9, 11, 15, 23, 25\}.$$

**Remark 6.** Fix $q$ a prime number such that $q = 8l + 7$ for some nonnegative integer $l$. It follows from the law of quadratic residues that $(\frac{2}{q}) = 1$, where $(\frac{2}{q})$ is the Legendre symbol. This implies that $(\frac{2t}{q}) = (\frac{t}{q})$, since the Legendre symbol is multiplicative. Thus $2t$ is a quadratic residue (respectively nonresidue) if and only if $t$ is a quadratic residue (respectively nonresidue).

**Lemma 7.** *With $m_1, n_1$ as in Remark 4,*

$$m_1 = n_1.$$

**Proof.** Define a function

$$g_1 : M_1 \to O \quad \text{by } g_1(t) = 2t.$$

From Remark 6, this function $g_1$ is a well-defined bijection. Thus $t \in K_2$ and $\frac{q+1}{2} \leqslant t \leqslant q-1$, i.e., $t \in M_1$ if and only if $2t$ is in $K_2$ and $2t-q$ is odd. This implies that the number of elements in $M_1$ is equal to the number of elements in $O$ as desired. □

**Remark 8.** Define a function

$$g_2 : \mathbf{K}_1 \cap (-\mathbf{K}_2) \to K_1 \times K_2, \quad \text{by } m \pmod e \mapsto (a, b),$$

where $m \equiv a \pmod 4$, $m \equiv -b \pmod q$. Then $g_2$ is a bijection by the Chinese Remainder Theorem. This implies that $\sharp(\mathbf{K}_1 \cap (-\mathbf{K}_2)) = (\sharp K_1)(\sharp K_2)$. Note that $\sharp(\mathbf{K}_1 \cap \mathbf{K}_2) = \sharp(\mathbf{K}_1 \cap (-\mathbf{K}_2)) = \frac{q-1}{2} = \frac{\phi(e)}{4}$.

**Proposition 9.** *The rational number $n_0$ is an integer.*

**Proof.** By Lemma 7 and Remark 8, $n_0 = \frac{1}{2}(m_1 + n_1) + \frac{S}{2} - \frac{3\phi(e)}{8} = n_1 + \frac{\phi(e)}{8} - \frac{3\phi(e)}{8} = n_1 - \frac{\phi(e)}{4} = n_1 - \frac{q-1}{2}$, which is an integer because of our choice for $q$. □

*2.2. Some lemmas*

For the remainder of this paper, we fix $a_1 = -1$, $a_2 = 2l+2$ such that

$$4a_2 + qa_1 = 1.$$

Then $qa_1 \equiv 1 \pmod 4$ and $4a_2 \equiv 1 \pmod q$. Let $s_1 = 4L_q(\sum_{t\in K_2} t)$ and let

$$A = \frac{1}{\prod_{t\in M_1} \tau(4t) \prod_{t\in O} \tau(2q+2t) \prod_{t\in I_3} \tau(4t)}, \tag{1}$$

$$B = \prod_{t\in O} \tau(q+t)\tau(3q+t) \prod_{t\in E} \tau(t)\tau(2q+t). \tag{2}$$

In [9], K. Yamamoto provided a formula for a sign ambiguity. We call it *Yamamoto's sign ambiguity*. We now reformulate his formula.

**Lemma 10.** *With $K_1$ as in Remark 4,*

$$\prod_{t\in K_1} DH_4^t = DH_4^1 = \chi^q(q)\chi(-1)p^{1-\frac{\phi(e)}{4}} \frac{\prod_{t\in \mathbf{K}_1} \tau(t)}{\tau(q)^2}.$$

**Proof.** Note that for integers $k$ and $t$, the congruence $k \equiv -a_2 t \pmod q$ is equivalent to $4k + t \equiv 0 \pmod q$, and when it holds, we have $4k + t \equiv a_1 qt = -qt \pmod e$.

Now consider the following (DH) relation for $e = mn$, $m = 4$, $n = q$ and $t \in K_1$:

$$
\begin{aligned}
DH_4^t &= \chi^{qt}(q)\frac{\tau(t)}{\tau(qt)}\prod_{k=1}^{q-1}\frac{\tau(4k+t)}{\tau(4k)}\\
&= \chi^{qt}(q)\frac{\tau(t)}{\tau(qt)}\,\frac{\tau(4+t)\tau(8+t)\ldots\tau(4(q-1)+t)}{\tau(4)\tau(8)\ldots\tau(4(q-1))}\\
&= \chi^{qt}(q)p^{-\frac{q-1}{2}}\frac{1}{\tau(qt)}\prod_{k=0}^{q-1}\tau(4k+t)\quad \text{by (NR)}\\
&= \frac{\chi^{qt}(q)p^{-\frac{q-1}{2}}}{\tau(qt)}\tau(a_1qt)\prod_{\substack{k=0\\ 4k+t\not\equiv 0 \pmod q}}^{q-1}\tau(4k+t)\\
&= \chi^{qt}(q)p^{-\frac{q-1}{2}}\frac{p\chi^{qt}(-1)}{\tau(qt)^2}\prod_{\substack{k=0\\ 4k+t\not\equiv 0 \pmod q}}^{q-1}\tau(4k+t)\quad \text{by (NR).}
\end{aligned}
$$

Note that

$$
\prod_{t\in K_1}\prod_{\substack{k=0\\ 4k+t\not\equiv 0 \pmod q}}^{q-1}\tau(4k+t)=\prod_{t\in\mathbf{K}_1}\tau(t).
$$

Since $K_1=\{1\}$,

$$
\begin{aligned}
\prod_{t\in K_1}DH_4^t &= \prod_{t\in K_1}\chi^{qt}(q)\chi(-1)p^{1-\frac{\phi(e)}{4}}\frac{1}{\tau(qt)^2}\prod_{t\in\mathbf{K}_1}\tau(t)\\
&= \chi^{q}(q)\chi(-1)p^{1-\frac{\phi(e)}{4}}\frac{\prod_{t\in\mathbf{K}_1}\tau(t)}{\tau(q)^2}. \qquad \square
\end{aligned}
$$

Similarly, we consider the (DH) relations when $e=mn$, $m=q$, $n=4$ and $t\in K_2$.

**Lemma 11.** *With $B$, $K_2$ as in Eq. (2), Remark 4, recall $s_1=4L_q(\sum_{t\in K_2}t)$ and let*

$$
J=\frac{B}{\prod_{t\in K_2}\tau(4t)}. \tag{3}
$$

*Then we have*

$$
\prod_{t\in K_2}DH_q^t=\chi^{s_1}(4)\chi(-1)p^{\frac{1}{2}-\frac{3\phi(e)}{8}}\cdot J\cdot\frac{\prod_{t\in\mathbf{K}_2}\tau(t)}{\tau(2q)}. \tag{4}
$$

**Proof.** Note that for integers $k$ and $t$, $k\equiv -a_1t\ (=t) \pmod 2 \Leftrightarrow qk+t\equiv 0 \pmod 2$. We consider two different cases of the (DH) relations up to the parity of $t$ in $K_2$ and of $k$ in $\{0,1,2,3\}$, since $qk+t\equiv 0 \pmod 2$ if and only if either $t$ is odd, $k\in\{1,3\}$ or $t$ is even, $k\in\{0,2\}$.

Case (1): $t$ is an odd integer in $K_2$;

$$\begin{aligned} DH_q^{\mathrm{odd}\ t} &= \chi^{4t}(4)\frac{\tau(t)}{\tau(4t)}\prod_{k=1}^{3}\frac{\tau(kq+t)}{\tau(kq)} \\ &= \chi^{4t}(4)\frac{\tau(t)}{\tau(4t)}\frac{\tau(q+t)\tau(2q+t)\tau(3q+t)}{\tau(q)\tau(2q)\tau(3q)} \\ &= \chi^{4t}(4)\frac{\chi^q(-1)p^{-1}}{\tau(4t)\tau(2q)}\prod_{k=0}^{3}\tau(kq+t) \quad \text{by (NR)} \\ &= \chi^{4t}(4)\frac{\chi(-1)p^{-1}\tau(q+t)\tau(3q+t)}{\tau(4t)\tau(2q)} \prod_{\substack{k=0 \\ kq+t\not\equiv 0 \pmod 2}}^{3}\tau(kq+t). \end{aligned}$$

Case (2): $t$ is an even integer in $K_2$; Similarly, we have

$$DH_q^{\mathrm{even}\ t} = \chi^{4t}(4)\frac{\chi(-1)p^{-1}\tau(t)\tau(2q+t)}{\tau(4t)\tau(2q)} \prod_{\substack{k=0 \\ kq+t\not\equiv 0 \pmod 2}}^{3}\tau(kq+t).$$

Note that

$$\prod_{t\in K_2}\prod_{\substack{k=0 \\ kq+t\not\equiv 0 \pmod 2}}^{3}\tau(kq+t) = \prod_{t\in \mathbf{K}_2}\tau(t) \tag{5}$$

and that

$$\prod_{t\in K_2}\tau(2q) = \tau(2q)^{\#K_2} = \tau(2q)p^{\frac{\phi(e)}{8}-\frac{1}{2}}. \tag{6}$$

Thus we have

$$\begin{aligned} \prod_{t\in K_2} DH_q^t &= \prod_{t\in O}\left(\chi(4)^{4t}\frac{\chi(-1)p^{-1}\tau(q+t)\tau(3q+t)}{\tau(4t)\tau(2q)} \prod_{\substack{k=0 \\ kq+t\not\equiv 0 \pmod 2}}^{3}\tau(kq+t)\right) \\ &\quad\cdot\prod_{t\in E}\left(\chi(4)^{4t}\frac{\chi(-1)p^{-1}\tau(t)\tau(2q+t)}{\tau(4t)\tau(2q)} \prod_{\substack{k=0 \\ kq+t\not\equiv 0 \pmod 2}}^{3}\tau(kq+t)\right) \\ &= \chi(-1)^{\#K_2}\cdot p^{-\#K_2}\cdot J\prod_{t\in K_2}\frac{\chi(4)^{4t}}{\tau(2q)}\prod_{t\in K_2}\prod_{\substack{k=0 \\ kq+t\not\equiv 0 \pmod 2}}^{3}\tau(kq+t) \\ &= \chi(-1)\cdot p^{-\frac{\phi(e)}{4}-(\frac{\phi(e)}{8}-\frac{1}{2})}\cdot J\cdot\frac{\chi(4)^{4\sum_{t\in K_2}t}}{\tau(2q)}\prod_{t\in \mathbf{K}_2}\tau(t) \quad \text{by Eqs. (5), (6)} \end{aligned}$$

$$= \chi(4)^{s_1} \cdot \chi(-1) \cdot p^{\frac{1}{2}-\frac{3\phi(e)}{8}} \cdot J \cdot \frac{\prod_{t\in\mathbf{K}_2}\tau(t)}{\tau(2q)}. \qquad \square$$

**Lemma 12.**

$$\prod_{t\in\mathbf{K}_1}\tau(t)\prod_{t\in\mathbf{K}_2}\tau(t) = \chi(-1)^{\sum_{t\in\mathbf{K}_1\cap(-\mathbf{K}_2)}t} p^{\sharp(\mathbf{K}_1\cap(-\mathbf{K}_2))}\prod_{t\in\mathbf{K}_1\cap\mathbf{K}_2}\tau(t)^2.$$

**Proof.** Note that $\mathbf{K}_1$, $\mathbf{K}_2$ are also half-sets of $G$ and that $\prod_{t\in(-\mathbf{K}_1)\cap\mathbf{K}_2}\tau(t) = \prod_{-t\in\mathbf{K}_1\cap(-\mathbf{K}_2)}\tau(t) = \prod_{t\in\mathbf{K}_1\cap(-\mathbf{K}_2)}\tau(-t) = \prod_{t\in\mathbf{K}_1\cap(-\mathbf{K}_2)}\frac{p\chi^t(-1)}{\tau(t)}$.

$$\begin{aligned}
\prod_{t\in\mathbf{K}_1}\tau(t)\prod_{t\in\mathbf{K}_2}\tau(t) &= \prod_{t\in\mathbf{K}_1\cap\mathbf{K}_2}\tau(t)\prod_{t\in(-\mathbf{K}_1)\cap\mathbf{K}_2}\tau(t)\prod_{t\in\mathbf{K}_1\cap\mathbf{K}_2}\tau(t)\prod_{t\in\mathbf{K}_1\cap(-\mathbf{K}_2)}\tau(t)\\
&= \prod_{t\in\mathbf{K}_1\cap(-\mathbf{K}_2)}\frac{p\chi^t(-1)}{\tau(t)}\prod_{t\in\mathbf{K}_1\cap(-\mathbf{K}_2)}\tau(t)\prod_{t\in\mathbf{K}_1\cap\mathbf{K}_2}\tau(t)^2\\
&= \prod_{t\in\mathbf{K}_1\cap(-\mathbf{K}_2)}\frac{\chi^t(-1)p\tau(t)}{\tau(t)}\prod_{t\in\mathbf{K}_1\cap\mathbf{K}_2}\tau(t)^2\\
&= \chi(-1)^{\sum_{t\in\mathbf{K}_1\cap(-\mathbf{K}_2)}t} p^{\sharp(\mathbf{K}_1\cap(-\mathbf{K}_2))}\prod_{t\in\mathbf{K}_1\cap\mathbf{K}_2}\tau(t)^2. \qquad \square
\end{aligned}$$

**Lemma 13.** *With $E$, $O$ as in Remark 4,*

$$\prod_{h\in E}\tau(2h)\prod_{s\in O}\tau(2q-2s) = \prod_{1\leqslant t\leqslant\frac{q-1}{2}}\tau(4t). \tag{7}$$

**Proof.** Let $h\in E$. Then there exists $t$, $t\in I_1$ such that $h = 2t$ by Remark 6. This implies that $2h = 2(2t) = 4t$. From Lemma 7 every odd integer $s$ in $K_2$ can be represented as $s = 2t - q$, where $t\in M_1$. Thus $2(q-s) = 2(q-(2t-q)) = 4(q-t)$ and $q-t\ (\equiv -t \pmod q)\in I_2$. $\square$

**Lemma 14.** *With $A$ as in* (1)*, let*

$$D = \frac{1}{\prod_{t\in K_2}\tau(4t)\prod_{t\in O}\tau(2q+2t)\prod_{t\in E}\tau(2t)}.$$

*Then we have*

$$D = \left(p^{\frac{m_1+n_1}{2}}A\right)^2.$$

**Proof.** Let

$$D_1 = \frac{1}{\prod_{t\in K_2}\tau(4t)} \quad\text{and}\quad D_2 = \frac{1}{\prod_{t\in O}\tau(2q+2t)\prod_{t\in E}\tau(2t)}.$$

By using the norm relation, we can rewrite $D_1$:

$$D_1 = \frac{1}{\prod_{t\in K_2}\tau(4t)} = \frac{1}{\prod_{t\in M_1}\tau(4t)\prod_{t\in I_1}\tau(4t)}$$
$$= \frac{p^{m_1}}{(\prod_{t\in M_1}\tau(4t))^2\prod_{t\in M_1}\tau(4q-4t)\prod_{t\in I_1}\tau(4t)}$$
$$= \frac{p^{m_1}}{(\prod_{t\in M_1}\tau(4t))^2\prod_{t\in I_3}\tau(4t)} \quad \text{by Lemma 13.}$$

Similarly, we can replace $D_2$:

$$D_2 = \frac{1}{\prod_{t\in O}\tau(2q+2t)\prod_{t\in E}\tau(2t)}$$
$$= \frac{p^{n_1}}{(\prod_{t\in O}\tau(2q+2t))^2\prod_{t\in O}\tau(2q-2t)\prod_{t\in E}\tau(2t)}$$
$$= \frac{p^{n_1}}{(\prod_{t\in O}\tau(2q+2t))^2\prod_{t\in I_3}\tau(4t)} \quad \text{by Lemma 13.}$$

Thus we have

$$D = \frac{p^{m_1}}{(\prod_{t\in M_1}\tau(4t))^2\prod_{t\in I_3}\tau(4t)}\cdot\frac{p^{n_1}}{(\prod_{t\in O}\tau(2q+2t))^2\prod_{t\in I_3}\tau(4t)}$$
$$= \left(\frac{p^{\frac{m_1+n_1}{2}}}{\prod_{t\in M_1}\tau(4t)\prod_{t\in O}\tau(2q+2t)\prod_{t\in I_3}\tau(4t)}\right)^2. \qquad \square$$

Finally, we will consider the following types of the (DH) relations when $m = 2q$, $n = 2$: For an odd $t$ in $K_2$,

$$DH_{2q}^{q+t} = \chi^{2q+2t}(2)\frac{\tau(q+t)\tau(3q+t)}{\tau(2q+2t)\tau(2q)}$$

and for an even $t$ in $K_2$,

$$DH_{2q}^{t} = \chi^{2t}(2)\frac{\tau(t)\tau(2q+t)}{\tau(2t)\tau(2q)}.$$

**Lemma 15.** *With $A$, $B$ and $J$ as in* (1), (2), (3), *let*

$$T = J\cdot\prod_{t\in O}DH_{2q}^{q+t}\prod_{t\in E}DH_{2q}^{t}.$$

*Then we have*

$$T = \frac{p^{\frac{1}{2}-\frac{\phi(e)}{8}+m_1+n_1}}{\tau(2q)}\left(\chi(2)^{qn_1+\sum_{t\in K_2}t}AB\right)^2.$$

**Proof.**

$$
\begin{aligned}
T &= \frac{\prod_{t\in O}\tau(q+t)\tau(3q+t)\prod_{t\in E}\tau(t)\tau(2q+t)}{\prod_{t\in K_2}\tau(4t)}\prod_{t\in O}DH_{2q}^{q+t}\prod_{t\in E}DH_{2q}^{t}\\
&= \frac{\prod_{t\in O}DH_{2q}^{q+t}\tau(q+t)\tau(3q+t)\prod_{t\in E}DH_{2q}^{t}\tau(t)\tau(2q+t)}{\prod_{t\in K_2}\tau(4t)}\\
&= \frac{1}{\prod_{t\in K_2}\tau(4t)}\prod_{t\in O}\left(\chi^{2q+2t}(2)\frac{\tau(q+t)\tau(3q+t)}{\tau(2q+2t)\tau(2q)}\tau(q+t)\tau(3q+t)\right)\\
&\quad\cdot\prod_{t\in E}\left(\chi^{2t}(2)\frac{\tau(t)\tau(2q+t)}{\tau(2t)\tau(2q)}\tau(t)\tau(2q+t)\right)\\
&= \frac{\chi(2)^{2qn_1+2\sum_{t\in K_2}t}}{\tau(2q)^{\#K_2}\prod_{t\in K_2}\tau(4t)}\prod_{t\in O}\frac{\tau(q+t)^2\tau(3q+t)^2}{\tau(2q+2t)}\prod_{t\in E}\frac{\tau(t)^2\tau(2q+t)^2}{\tau(2t)}\\
&= \frac{\chi(2)^{2qn_1+2\sum_{t\in K_2}t}p^{\frac{1}{2}-\frac{\phi(e)}{8}}D}{\tau(2q)}\left(\prod_{t\in O}\tau(q+t)\tau(3q+t)\prod_{t\in E}\tau(t)\tau(2q+t)\right)^2\\
&= \frac{p^{\frac{1}{2}-\frac{\phi(e)}{8}+m_1+n_1}}{\tau(2q)}\left(\chi(2)^{qn_1+\sum_{t\in K_2}t}AB\right)^2 \quad \text{by Lemma 14.} \qquad \square
\end{aligned}
$$

*2.3. Yamamoto's sign ambiguity*

Let $R_e$ be the set of quadratic residues modulo $e$ in $G$. Note that

$$\mathbf{K}_1\cap\mathbf{K}_2 = R_e,$$

see [4, Proposition 5.1.1]. In other words, an integer $t$ is a quadratic residue modulo 4 and modulo $q$ if and only if $t$ is also a quadratic residue modulo $e$. Recall $A, B$ and $n_0$ from Eqs. (1), (2) and Remark 4. Define

$$Y = \frac{p^{n_0}\tau(2q)ABC\prod_{t\in R_e}\tau(t)}{\tau(q)} \tag{8}$$

where

$$C = \chi^{\frac{q}{2}}(q)\chi(2)^{s_1+qn_1+\sum_{t\in K_2}t}\chi(-1)^{\frac{1}{2}\sum_{t\in\mathbf{K}_1\cap(-\mathbf{K}_2)}t}.$$

**Theorem 16.**

$$Y = \pm 1.$$

**Proof.** Recall $DH_m^t = 1$ for $1\leqslant t\leqslant m-1$. We will show how $Y^2 = 1$ is a consequence of the (DH) relations.

$$1 = \prod_{t\in K_1}DH_4^t\prod_{t\in K_2}DH_q^t\prod_{t\in O}DH_{2q}^{q+t}\prod_{t\in E}DH_{2q}^{t}$$

$$= \chi^q(q)\chi(-1)p^{1-\frac{\phi(e)}{4}}\frac{\prod_{t\in\mathbf{K}_1}\tau(t)}{\tau(q)^2} \quad \text{by Eq. (4), Lemma 10}$$

$$\cdot \chi^{s_1}(4)\chi(-1)p^{\frac{1}{2}-\frac{3\phi(e)}{8}}\cdot J\cdot\frac{\prod_{t\in\mathbf{K}_2}\tau(t)}{\tau(2q)}\prod_{t\in O}DH_{2q}^{q+t}\prod_{t\in E}DH_{2q}^{t}$$

$$= \chi^q(q)\chi^{s_1}(4)p^{\frac{3}{2}-\frac{5\phi(e)}{8}}\cdot T\cdot\frac{\prod_{t\in\mathbf{K}_1}\tau(t)\prod_{t\in\mathbf{K}_2}\tau(t)}{\tau(2q)\tau(q)^2} \quad \text{by Lemma 15}$$

$$= \chi^q(q)\chi^{2s_1}(2)p^{\frac{3}{2}-\frac{5\phi(e)}{8}}\frac{p^{\frac{1}{2}-\frac{\phi(e)}{8}+m_1+n_1}}{\tau(2q)}\big(\chi(2)^{qn_1+\sum_{t\in K_2}t}AB\big)^2$$

$$\cdot\left(\frac{\prod_{t\in\mathbf{K}_1}\tau(t)\prod_{t\in\mathbf{K}_2}\tau(t)}{\tau(2q)\tau(q)^2}\right) \quad \text{by Lemma 15}$$

$$= \chi^q(q)\chi(2)^{2s_1+2qn_1+2(\sum_{t\in K_2}t)}\chi(-1)^{\sum_{t\in\mathbf{K}_1\cap(-\mathbf{K}_2)}t}p^{2-\frac{3\phi(e)}{4}+m_1+n_1+S}$$

$$\cdot\left(\frac{AB\prod_{t\in\mathbf{K}_1\cap\mathbf{K}_2}\tau(t)}{\tau(2q)\tau(q)}\right)^2 \quad \text{by Lemma 12}$$

$$= \left(\frac{p^{n_0}\tau(2q)ABC\prod_{t\in R_e}\tau(t)}{\tau(q)}\right)^2 \quad \text{by (NR).} \qquad \square$$

Thus we showed that the square of $Y$ depends on the (DH) relations as desired. This induces the following theorem.

**Theorem 17.** *The equation $Y = \pm 1$ is a sign ambiguity.*

**Proof.** In [9], K. Yamamoto proved that $Y = \pm 1$ is a multiplicatively independent relationship of Gauss sums which is not direct consequences of the norm and the Davenport–Hasse relations and that it is a sign ambiguity up to a power of $p$ and a unit. $\square$

## 3. Main result

We are interested in the problem of writing down sign ambiguities and also explicitly describing the sign in such identities. In this section we give formula to determine whether $Y$ is 1 or $-1$.

### 3.1. Explicit signs

In Theorem 19 we explicitly determine the signs of sign ambiguities by using Stickelberger's congruence for Gauss sums, see [1, Theorem 11.2.1]. Recall that $p \equiv 1 \pmod{e}$. Let

$$f = \frac{p-1}{e} = \frac{p-1}{4q}.$$

For the remainder of this paper we restrict $p$ so that $f$ is even, i.e., $p \equiv 1 \pmod{2e}$.

**Lemma 18.** *For all $a \in \{1, 2, \ldots, e-1\}$,*

$$(fa)!\big(f(e-a)\big)! \equiv -1 \pmod{p}.$$

**Proof.**

$$\begin{aligned}\big(f(e-a)\big)! &= 1\cdot 2\cdot 3\cdots f(e-a)\\ &\equiv (-1)^{f(e-a)}(p-1)(p-2)\cdots\big(p-f(e-a)\big) \pmod p\\ &= (fe)(fe-1)\cdots(1+fa) \quad \text{since } f \text{ is even.}\end{aligned}$$

Thus we have

$$\begin{aligned}\big(f(e-a)\big)!(fa)! &\equiv (fe)(fe-1)\cdots(1+fa)(fa)! \pmod p\\ &= (p-1)!\\ &\equiv -1 \pmod p \quad \text{by Wilson's theorem.} \qquad \square\end{aligned}$$

Note that $\chi(-1)^{\frac{1}{2}\sum_{t\in \mathbf{K}_1\cap(-\mathbf{K}_1)}t} = \chi(\gamma^{\frac{p-1}{2}})^{\frac{1}{2}\sum_{t\in \mathbf{K}_1\cap(-\mathbf{K}_1)}t} = \chi(\gamma)^{fq\sum_{t\in \mathbf{K}_1\cap(-\mathbf{K}_1)}t}$, because $\gamma^{\frac{p-1}{2}} \equiv -1 \pmod p$.

Let $\mathcal{O}_{\mathbb{M}} \subseteq \mathcal{O}_{\mathbb{E}}$ be rings of integers of the number fields $\mathbb{M} = \mathbb{Q}(\zeta_e)$, $\mathbb{E} = \mathbb{Q}(\zeta_{ep})$ respectively. Let $\mathfrak{P} \subseteq \mathcal{O}_{\mathbb{M}}$ be the prime ideal dividing (i.e., containing) the principal ideal $p\mathcal{O}_{\mathbb{M}}$ such that $\chi$ can be identified with the power residue character modulo $\mathfrak{P}$, see [7, Theorem 3], that is, for an integer $a$ we have

$$\chi(a) \equiv a^f \pmod{\mathfrak{P}}.$$

Let $\wp$ be the unique prime ideal of $\mathcal{O}_{\mathbb{E}}$ such that

$$\mathfrak{P}\mathcal{O}_{\mathbb{E}} = \wp^{p-1}, \quad \wp \cap \mathcal{O}_{\mathbb{M}} = \mathfrak{P}$$

(i.e., $\mathfrak{P}$ ramifies totally in $\mathcal{O}_{\mathbb{E}}$); see [6, p. 423].

**Theorem 19.** *Let $s(a) = L_e(a)f$ and $t(a) = (L_e(a)f)!$. Then we can explicitly determine the sign of $Y$ for each prime $p$, $p \equiv 1 \pmod{2e}$, from the following congruence*

$$Y \equiv \frac{(-1)^{n_0} N B' t(2q)\prod_{a\in R_e} t(a)}{t(q)\prod_{a\in M_1} t(4a)\prod_{a\in O} t(2q+2a)\prod_{a\in I_3} t(4a)} \pmod p,$$

*where*

$$N = q^{\frac{fq}{2}}\gamma^{\frac{f(p-1)}{4}\left(\sum_{t\in \mathbf{K}_1\cap(-\mathbf{K}_2)} t\right)} 2^{f\left(s_1+qn_1+\sum_{t\in K_2} t\right)}$$

*and*

$$B' = \prod_{a\in O} t(q+a)t(3q+a)\prod_{a\in E} t(a)t(2q+a).$$

**Proof.** Let $\pi = \zeta_p - 1$. Then we have, see [1, p. 343],

$$p\mathcal{O}_{\mathbb{E}} = \pi^{p-1}\mathcal{O}_{\mathbb{E}}, \qquad \pi\mathcal{O}_{\mathbb{E}} = \prod_{j\in(\mathbb{Z}/e\mathbb{Z})^\times} \wp_j.$$

From Stickelberger's congruence for Gauss sums, see [1, Theorem 11.2.1], for an integer $a$ $(1 \leqslant a \leqslant e-1)$, we have

$$\tau(a) \equiv \frac{-\pi^{f(e-a)}}{(f(e-a))!} \pmod{\wp^{s(-a)+1}},$$

and

$$\wp^{s(-a)} \parallel \tau(a)\mathcal{O}_{\mathbb{E}}, \tag{9}$$

where $\parallel$ means that the largest power of $\wp$ dividing $\tau(a)\mathcal{O}_{\mathbb{E}}$ is $s(-a)$. From Eq. (9), we can find all powers of $\wp$ dividing Gauss sums which are involved in $Y$. For example, $s(-2q) = s(2q)$ is the power of $\wp$ which divides $\tau(2q)$ in $Y$. Note that $\wp^{p-1} = \wp^{s(-a)}\wp^{s(a)} | p$ by using the norm relation. This implies that $\wp^{n_0(p-1)} | p^{n_0}$. Note that $Y = \pm 1$ is a unit and $\wp^w$ must divide $Y$, i.e., $w = 0$, where $w$ is given by the following equation:

$$w = (p-1)n_0 + s(2q) + \sum_{a\in O}\big[s(3q-a) + s(q-a)\big] + \sum_{a\in E}\big[s(-a) + s(2q-a)\big]$$
$$+ \sum_{a\in \mathbf{K}_1\cap\mathbf{K}_2} s(-a) - s(3q) - \sum_{a\in M_1} s(-4a) - \sum_{a\in O} s(2q-2a) - \sum_{a=1}^{\frac{q-1}{2}} s(-4a).$$

From Lemma 18, we have

$$\tau(a) \equiv \pi^{f(e-a)}(fa)! = \pi^{s(-a)}t(a) \pmod{\wp^{s(-a)+1}},$$

where $1 \leqslant a \leqslant e-1$. Note that $p \equiv -\pi^{p-1} \pmod{\wp^p}$ by applying Eq. (9) to the norm relation, and that the principal ideal $(\pi)$ in $\mathbb{Z}[\zeta_p]$ is prime, since $\pi$ has prime norm $p$, see [1, Theorem 2.1.9]. Now we have the following congruence modulo $\wp$ of $Y$, see [1, Theorem 11.2.10],

$$Y \equiv \frac{(-1)^{n_0} N B' t(2q) \prod_{a\in R_e} t(a)}{t(q)\prod_{a\in M_1} t(4a)\prod_{a\in O} t(2q+2a)\prod_{a\in I_3} t(4a)} \pmod{\wp}.$$

As $Y$ and the values of $\chi$ are in $\mathcal{O}_{\mathbb{M}}$, this congruence holds modulo $\mathfrak{P}$. Using $\chi^i(a) \equiv a^{fi} \pmod{\mathfrak{P}}$ we get a congruence involving only rationals and the theorem follows. □

### 3.2. Sign ambiguities

We have revised Yamamoto's sign ambiguities, see [9, Lemma 9] for fixed half-sets and explicitly determined their signs in Theorem 16 and Theorem 19.

**Lemma 20.** *With $K_2$, $O$ and $E$ as in Remark 4, we have*

$$\prod_{t\in K_2}\tau(2t) = \prod_{t\in O}\tau(q+t)\prod_{t\in E}\tau(t),$$
$$\prod_{t\in K_2}\tau(2q+2t) = \prod_{t\in O}\tau(3q+t)\prod_{t\in E}\tau(2q+t).$$

**Proof.** Note that $K_2 = I_1 \cup M_1$. For any $t$ in $M_1$, there is an odd number $a \in O$ such that $q + a = 2t$ from Lemma 7. From Remark 6. $t \in I_1$ implies that $2t$ is also in $K_2$ and is even. Therefore

$$\begin{aligned}\prod_{t\in K_2} \tau(2t) &= \prod_{t\in M_1} \tau(2t) \prod_{t\in I_1} \tau(2t)\\ &= \prod_{t\in O} \tau(q+t) \prod_{t\in E} \tau(t).\end{aligned}$$

The second equation follows from the first equation by adding $2q$. □

**Lemma 21.**

$$\sharp(R_e) = n_1 - n_0.$$

**Proof.** From the reformulated Remark 8 and Proposition 9,

$$\sharp(R_e) = \sharp(\mathbf{K}_1 \cap \mathbf{K}_2) = \frac{q-1}{2} = n_1 - n_0. \qquad \square$$

**Lemma 22.**

$$\prod_{a\in O} \tau(2q+2a) \prod_{b\in M_1} \tau(4q-4b) = p^{n_1}.$$

**Proof.** From Lemma 7, there exists a number $a \in O$ such that $2b = q + a$ for some $b \in M_1$. Thus we have $4q - 4b = 4q - 2(q + a) = 2q - 2a$. So by the norm relation, we can replace each term by the character value times $p$. For example, $\tau(2q+2a)\tau(4q-4b) = \tau(2q+2a)\tau(2q-2a) = \chi^{2q+2a}(-1)p = p$ since $2q + 2a$ is even. □

**Lemma 23.**

$$\prod_{s\in R_e} \tau(4q-2s) = \prod_{t\in K_2} \frac{\tau(4q-2t)\tau(2q-2t)}{\tau(4q-4t)}.$$

**Proof.** Note that $s \in R_e$ can be written as $s = kq + t$, where $k \in \{0, 1, 2, 3\}$, $t \in K_2$, and that either $k \in \{0, 2\}$, $t \in O$ or $k \in \{1, 3\}$, $t \in E$. Thus there are two possible cases for $s$.

Case (1): $s = t$ or $s = 2q + t \Rightarrow 4q - 2s \equiv 4q - 2t \pmod{e}$.

Case (2): $s = q + t$ or $s = 3q + t \Rightarrow 4q - 2s \equiv 2q - 2t \pmod{e}$

$$\begin{aligned}\prod_{s\in R_e} \tau(4q-2s) &= \prod_{t\in O} \tau(4q-2t) \prod_{t\in E} \tau(2q-2t)\\ &= \frac{\prod_{t\in K_2} \tau(4q-2t)\tau(2q-2t)}{\prod_{t\in E} \tau(4q-2t) \prod_{t\in O} \tau(2q-2t)}\\ &= \prod_{t\in K_2} \frac{\tau(4q-2t)\tau(2q-2t)}{\tau(4q-4t)} \quad \text{by Lemma 13.} \qquad \square\end{aligned}$$

Define the following subset $\Omega$ of $G = (\mathbb{Z}/e\mathbb{Z})^\times$,

$$\Omega = R_e \cup \{3q\}. \tag{10}$$

Let

$$K = \frac{\chi(-1)C\prod_{t\in\Omega}\tau(t)}{\prod_{t\in\Omega}\tau(2t)} = \frac{\chi(-1)C\tau(3q)\prod_{t\in R_e}\tau(t)}{\tau(2q)\prod_{t\in R_e}\tau(2t)}. \tag{11}$$

**Theorem 24.** *With Yamamoto's sign ambiguity $Y$ as defined in Eq.* (8) *and $K$ as defined in Eq.* (11)*, the following equation holds*:

$$\frac{K}{Y} = \frac{\prod_{t\in(-K_2)} DH_{2q}^{2t}}{\prod_{t\in K_2} DH_{2q}^{2t}} = 1.$$

**Proof.**

$$\begin{aligned}
\frac{K}{Y} &= \frac{\chi(-1)C\tau(q)\prod_{t\in\Omega}\tau(t)}{Cp^{n_0}\tau(2q)AB\prod_{t\in R_e}\tau(t)\prod_{t\in\Omega}\tau(2t)} \quad \text{by Eqs. (8), (11)}\\
&= \frac{\prod_{t\in M_1}\tau(4t)\prod_{t\in O}\tau(2q+2t)\prod_{t\in I_3}\tau(4t)}{p^{n_0}\prod_{t\in O}\tau(q+t)\tau(3q+t)\prod_{t\in E}\tau(t)\tau(2q+t)\prod_{t\in R_e}\tau(2t)} \quad \text{by (NR)}\\
&= \frac{p^{n_1-n_0}\prod_{t\in K_2}\tau(4t)}{\prod_{t\in R_e}\tau(2t)\prod_{t\in K_2}\tau(2t)\tau(2q+2t)} \quad \text{by Lemmas 20, 22}\\
&\quad \text{Note that } K_2 = I_1\cup M_1 \text{ and } \prod_{t\in I_2}\tau(4t) = \prod_{t\in M_1}\tau(4q-4t)\\
&= \prod_{t\in K_2}\frac{\tau(4t)}{\tau(2t)\tau(2q+2t)}\prod_{t\in R_e}\tau(4q-2t) \quad \text{by (NR)}\\
&= \prod_{t\in K_2}\frac{\tau(4t)}{\tau(2t)\tau(2q+2t)}\prod_{t\in K_2}\frac{\tau(4q-2t)\tau(2q-2t)}{\tau(4q-4t)} \quad \text{by Lemma 23}\\
&= \prod_{t\in K_2}\frac{\tau(4t)}{\tau(2t)\tau(2q+2t)}\prod_{t\in(-K_2)}\frac{\tau(2t)\tau(2q+2t)}{\tau(4t)}\\
&= \frac{\prod_{t\in(-K_2)}\frac{\tau(2t)\tau(2q+2t)}{\tau(4t)}}{\prod_{t\in K_2}\frac{\tau(2t)\tau(2q+2t)}{\tau(4t)}}\\
&= \frac{\prod_{t\in(-K_2)}\chi^{4t}(2)\frac{\tau(2t)\tau(2q+2t)}{\tau(4t)\tau(2q)}}{\prod_{t\in K_2}\chi^{4t}(2)\frac{\tau(2t)\tau(2q+2t)}{\tau(4t)\tau(2q)}}\\
&= \frac{\prod_{t\in(-K_2)}DH_{2q}^{2t}}{\prod_{t\in K_2}DH_{2q}^{2t}} = 1 \quad \text{by (DH).} \qquad \square
\end{aligned}$$

We now state our main theorem.

**Theorem 25.** *Let $e = 4q$ with a prime $q \equiv 7 \pmod 8$, and let $p$ be a prime such that $p \equiv 1 \pmod{2e}$. Let $Y$ and $K$ be as in Eqs.* (8), (11)*. Then the equation $K = \pm 1$ is a sign ambiguity. We explicitly determine the sign by Theorem* 19 *as follows*:

$$K \equiv \frac{(-1)^{n_0}Nt(2q)B'\prod_{a\in R_e}t(a)}{t(q)\prod_{a\in M_1}t(4a)\prod_{a\in O}t(2q+2a)\prod_{a\in I_3}t(4a)} \pmod p,$$

*where*

$$n_0 = \frac{1}{2}\big(\sharp(\mathbf{K}_1 \cap (-\mathbf{K}_2)) + m_1 + n_1\big) - \frac{3\phi(e)}{8},$$
$$N = q^{\frac{fq}{2}} \gamma^{\frac{f(p-1)}{4}(\sum_{t\in \mathbf{K}_1\cap(-\mathbf{K}_2)} t)} 2^{f(s_1+qn_1+\sum_{t\in K_2} t)}$$

*and*

$$B' = \prod_{a\in O} t(q+a)t(3q+a) \prod_{a\in E} t(a)t(2q+a).$$

**Proof.** The proof of this theorem is the immediate consequence of Theorems 24, 19 and 16. □

**Definition 26.** If $n$ is an integer not divisible by $p$, then the unique integer $t$ such that

$$n \equiv \gamma^t \pmod{p}, \quad 0 \leqslant t < p-1,$$

is called the index of $n$ with respect to the generator $\gamma$ of $\mathbb{F}_p^*$, and is denoted by $ind_\gamma n$.

Now we conclude with an example of our main theorem and provide Table 1 for ambiguous signs of $e = 28$ and prime numbers $p$ up to 10 000.

**Example 27.** Let $e = 28 = 4 \cdot 7$, $p$ be a prime such that $p \equiv 1 \pmod{2e}$, and let $K_1, K_2, \mathbf{K}_1, \mathbf{K}_2$ be as in Example 5. Recall that $\gamma$ is a generator of the cyclic group $\mathbb{F}_p^*$ and $\chi(\gamma) = \zeta_{28}$. Then with $\Omega$ as defined by Eq. (10), we have

$$\Omega = R_e \cup \{3q\} = \{1, 9, 21, 25\},$$

and Theorem 25 gives

$$K = \zeta_{28}^{\frac{7}{2}t_1 + 37(p-1)/4 + 14t_2} \frac{\prod_{t\in\Omega} \tau(t)}{\prod_{t\in\Omega} \tau(2t)} = \pm 1$$

is a sign ambiguity, and the sign is $+1$ if and only if

$$\frac{\gamma^{f(\frac{7}{2}t_1 + 35(p-1)/4 + 14t_2)}(14f)!(22f)!(2f)!(18f)!f!(9f)!(25f)!}{(7f)!(16f)!(12f)!} \equiv 1 \pmod{p}$$

and $-1$ otherwise, where $t_1 = ind_\gamma 7$ (i.e., $\gamma^{t_1} = 7$) and $t_2 = ind_\gamma 2$. By using magma [2] we compute the ambiguous signs for primes $p < 20\,000$, see Table 1.

## References


[1] B. Berndt, R. Evans, K. Williams, Gauss and Jacobi Sums, John Wiley and Sons, Inc., 1998.
[2] J.J. Cannon, W. Bosma (Eds.), Handbook of Magma Functions, edition 2.13, 2006, 4350 pp.
[3] H. Hasse, Vorlesungen über Zahlentheorie, 2nd ed., Springer-Verlag, Berlin, 1964.
[4] K. Ireland, M. Rosen, A classical Introduction to Modern Number Theory, Springer-Verlag, New York, 1990.
[5] B.J. Murray, Explicit multiplicative relations between Gauss sums, J. Number Theory 126 (1) (September 2007) 87–109.
[6] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, Springer-Verlag/PWN-Polish Scientific Publishers, Berlin, Warsaw, 1990.
[7] P. van Wamelen, New explicit multiplicative relations between Gauss sums, Int. J. Number Theory 3 (2) (2007) 275–292.

**Table 1**
Ambiguous signs for $e = 28$.

| $K = 1$ | $p = 337$ | 449 | 617 | 953 | 2297 | 2689 | 3697 | 4201 |
|---|---|---|---|---|---|---|---|---|
| | 4481 | 4817 | 5153 | 5209 | 6217 | 6329 | 6553 | 7001 |
| | 7057 | 7841 | 8233 | 9521 | 9689 | 10193 | 10529 | 10753 |
| | 11369 | 11593 | 12377 | 12713 | 13049 | 13217 | 14281 | 14449 |
| | 14561 | 14897 | 15233 | 16073 | 17137 | 17417 | 17977 | 18481 |
| | 18593 | 19433 | 19489 | 19937 | 19993 | | | |
| $K = -1$ | $p = 113$ | 281 | 673 | 1009 | 1289 | 2017 | 2129 | 2521 |
| | 2633 | 2801 | 2857 | 2969 | 3137 | 3361 | 4649 | 5657 |
| | 6833 | 7393 | 7561 | 7673 | 8009 | 8513 | 8681 | 8737 |
| | 8849 | 9241 | 11257 | 12041 | 12097 | 12433 | 12601 | 13441 |
| | 13553 | 13721 | 14057 | 15121 | 15289 | 15401 | 15569 | 15737 |
| | 16633 | 17921 | 18089 | 18257 | 18313 | | | |

[8] K. Yamamoto, On a conjecture of Hasse concerning multiplicative relations of Gaussian sums, J. Combin. Theory 1 (1966) 476–489.
[9] K. Yamamoto, The gap group of multiplicative relationships of Gaussian sums, in: Symposia Mathematica, vol. XV, Convegno di Strutture in Corpi Algebrici, INDAM, Rome, 1973, Academic Press, London, 1975, pp. 427–440.